GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Proteggere i dati per governare la complessità

Discorso del Presidente

Antonello Soro

Relazione2017

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Piazza di Monte Citorio, 121
00186 Roma
tel. 06 696771
e-mail: garante@gpdp.it
www.garanteprivacy.it

Relazione2017

Discorso del Presidente

Antonello Soro

Roma, 10 luglio 2018

Signor Presidente della Camera, Autorità, Signore e Signori,

Questa è la prima Relazione che il Garante presenta in un contesto normativo profondamente segnato dal nuovo quadro giuridico europeo, pienamente applicabile da poco più di un mese.

Si tratta di una disciplina fortemente innovativa, capace di adeguare il diritto ai profondi mutamenti generati dallo sviluppo delle nuove tecnologie: la prima, anche sul piano internazionale, che tenta di inscrivere in un sistema di regole democratiche la rivoluzione digitale.

Per molto tempo i governi, in ogni angolo del pianeta, hanno sottostimato gli effetti e i rischi di un regime privo di regolamentazione, nel quale i grandi gestori delle piattaforme del web hanno scritto le regole, promuovendo un processo inarrestabile di acquisizioni e concentrazioni, dando vita all'attuale sistema di oligopoli.

Questi hanno acquisito il potere di orientare i comportamenti di diversi miliardi di persone: non solo nei consumi ma anche nella più generale visione sociale e culturale.

E hanno guadagnato uno straordinario potere economico, per il ruolo di intermediari sempre più esclusivi tra produttori e consumatori e per le implicazioni che le tecnologie *data intensive*, l'intelligenza artificiale, la *big data analytics* hanno sulla dinamica dei mercati, al crocevia tra economia dell'informazione e della condivisione.

La distribuzione e la natura di questo potere hanno generato una inedita domanda di garanzie e, insieme, il timore di una progressiva riduzione degli spazi di libertà ed intimità individuale che hanno rappresentato il fondamento consolidato delle democrazie liberali del ventesimo secolo.

Il tempo dell'Internet of Me

È cresciuta la consapevolezza del fatto che non possono essere i protocolli informatici o le condizioni generali di contratto, unilateralmente stabilite dai *big tech*, il codice normativo del digitale, su cui fondare diritti e doveri, nel contesto in cui più di ogni altro si dispiega la nostra esistenza.

Proprio le straordinarie potenzialità delle nuove tecnologie esigono, infatti, uno statuto di regole capace di restituire alla persona quella centralità altrimenti negata dall'economia fondata sullo sfruttamento dei dati: materia prima di un nuovo capitalismo estrattivo alimentato da frammenti, spesso delicatissimi, della nostra vita.

In questo senso, l'assunzione da parte dell'Unione europea di un unico quadro normativo in tema di protezione dati - proprio in una fase storica in cui riemergono nazionalismi e spinte divisive e si fa più forte la tendenza a creare barriere alla libera circolazione di beni e persone - è una scelta densa di conseguenze politiche, che proietta l'Unione su una linea di avanguardia rispetto al governo della società digitale e della straordinaria complessità che la caratterizza.

Il nuovo quadro giuridico europeo ha, infatti, il merito di porre al centro dell'agenda politica le implicazioni del digitale sulla libertà, l'autodeterminazione, l'identità: definita, questa, sempre più a partire dalle caratteristiche che altri - nel nome del primato degli algoritmi - ci attribuiscono, scrivendo per noi la nostra storia.

Il caso recente di Cambridge Analytica - punta di un iceberg sicuramente ben più esteso - ha reso evidenti le implicazioni di ordine politico e ordinamentale della nuova geografia dei poteri delineata dal digitale.

L'ex amministratore delegato di CA, già nel 2016 dichiarava di disporre di "qualcosa di simile a 4-5 mila data point per ogni statunitense adulto", utilizzabili secondo un metodo che a suo dire sarebbe stato già applicato in "oltre duecento elezioni nel mondo".

Una parte rilevante delle inserzioni politiche veicolate online durante la

scorsa campagna presidenziale negli Stati Uniti parrebbe ascrivibile a gruppi sospetti, localizzati all'estero, che attraverso marketing politico personalizzato basato sulla profilazione, tentavano di condizionare l'esito delle elezioni.

È, in questo senso, significativo che la California abbia approvato e il Congresso degli Stati Uniti esamini un disegno di legge per l'introduzione di una disciplina privacy sul modello europeo, dopo aver compreso come l'assenza di regolazione possa consentire alle potenze straniere di condizionare, con un sapiente quanto spregiudicato uso della profilazione, persino il processo elettorale.

La mancanza di un quadro regolatorio adeguato, anziché favorire il libero dispiegarsi delle dinamiche di mercato e, con esse, il benessere collettivo, espone a rischio la stessa sovranità, rendendo vulnerabili proprio gli Stati che non hanno disciplinato le condizioni per un corretto sviluppo dell'economia digitale.

Molte sono le questioni aperte.

Fake news, hate speech, cyberbullismo, eterna memoria della rete, ma anche minacce cibernetiche, algoritmi predittivi, uso massivo dei big data, persuasione occulta e *social engineering* funzionale ad attacchi informatici. Questi ultimi in Italia, nel solo mese di maggio, hanno toccato la soglia di 140 al giorno. Dal 25 maggio sono aumentate di oltre il 500% le comunicazioni di *data breach* al Garante, che hanno interessato, assieme a quelli notificati a partire da marzo, oltre 330.000 persone.

D'altra parte, in un mondo dove tutto di noi sarà sempre più connesso, saremo sempre più vulnerabili, perché ogni oggetto con cui veniamo a contatto può diventare il canale di accesso per un attacco informatico, per una violazione della nostra persona.

Per questo è indispensabile fare della protezione dei dati una priorità delle politiche pubbliche.

Il ruolo di questo diritto e della sua tutela nella realtà attuale è, per altro verso, il portato di una società fondata sul potere della personalizzazione dei con-

tenuti proposti, al contrario dei mass media tradizionali, basati invece sull'universalità e unicità del servizio offerto.

Il web di cui facciamo esperienza non è, dunque, la rete, ma soltanto la sua parte selezionata da algoritmi che, analizzando le nostre attività e preferenze, ci espongono a contenuti il più possibile affini ad esse, per esigenze di massimizzazione dei ricavi da parte dei gestori, legate al tempo di permanenza e al traffico online.

Siamo dunque soggetti - più di quanto ne siamo consapevoli - a una sorveglianza digitale, in gran parte occulta, prevalentemente a fini commerciali e destinata, fatalmente, ad espandersi anche su altri piani, con effetti dirompenti sotto il profilo sociale.

La definizione "Internet of Me", riferita al flusso di dati che dalla rete giunge al singolo consumatore, con contenuti personalizzati, attraverso oggetti di uso quotidiano capaci di apprendere dall'esperienza e adattarsi in maniera evolutiva ai comportamenti, è in questo senso significativa.

Essa è infatti costruita su di un singolare ossimoro: internet dovrebbe essere il mondo, tutto ciò che è al di fuori di me e con cui "io" interagisco. Diviene invece la porzione di mondo che mi conferma nelle mie idee, la rappresentazione immateriale della realtà che mi sono costruito.

Algoritmi e libertà

Il legislatore europeo ha accolto e rilanciato la sfida del digitale delineando un quadro giuridico organico che, dal commerciale al giudiziario, dal lavoro alla ricerca scientifica, fornisce i criteri regolativi essenziali per beneficiare delle straordinarie opportunità dell'innovazione senza rinunciare alla libertà, all'autodeterminazione, persino all'eguaglianza: per scegliere liberamente e consapevolmente nella realtà digitale.

E si tratta di regole che hanno un impatto tutt'altro che irrilevante. Si pensi ai possibili effetti di una diffusa applicazione del diritto alla portabilità dei dati, che contrastando i fenomeni anticompetitivi del *lock-in* potrebbe scalfire l'intan-

gibilità degli oligopoli, soprattutto se accompagnata dall'interoperabilità dei sistemi, indispensabile ai fini pro-concorrenziali.

Un insieme di regole di portata innovativa che si dimostrano, in questa prospettiva, un efficacissimo presidio antitrust.

L'obiettivo di rendere l'innovazione un elemento di progresso anche sociale e umano è, del resto, il filo rosso sotteso ad ogni singola disposizione del Regolamento.

Tutto questo viene perseguito in un quadro che costituisce una nuova sfida per tutti gli operatori coinvolti, nel quale la tendenziale eliminazione di molti controlli preventivi è compensata dall'incorporazione nei trattamenti di misure di tutela e prevenzione del rischio, oltre che dalla più generale responsabilizzazione del titolare.

Al quale del resto sono riconosciute nuove possibilità di utilizzo dei dati, nell'economia dell'accesso - non più del possesso - con un rapporto tra consumatore e impresa molto più dinamico, nel quale si inseriscono nuove figure di lavoratori quali i protagonisti, sempre più vulnerabili, della *gig economy*.

E a fronte di tutto questo è significativo il rafforzamento dei diritti dell'interessato, anche rispetto alle applicazioni dell'intelligenza artificiale: tema che sta entrando finalmente nell'agenda politica.

Indicativo il fatto che il 10 aprile scorso 25 governi abbiano sottoscritto un accordo volto a sancire l'Alleanza Europea per l'Intelligenza Artificiale, decuplicando gli investimenti in ricerca, promuovendo una strategia per affrontarne l'impatto socio-economico e un codice etico fondato sul binomio responsabilità-sicurezza.

Sono infatti dirimenti le questioni etiche connesse alle varie applicazioni dell'intelligenza artificiale e al rapporto tra uomo e macchina: a partire dall'interrogativo se possa quest'ultima, del tutto indipendentemente dal suo creatore, assumere scelte proprie e imprevedibili, divenendo autonomo soggetto di diritto, centro di imputazione di responsabilità giuridica.

Dai veicoli a guida autonoma alle applicazioni predittive sulla salute: si pensi soltanto se possa un algoritmo decidere quale siano i pazienti meritevoli di cura e quali, invece, non lo siano per prognosi infausta.

Esiste uno stretto legame tra protezione dei dati e l'intelligenza artificiale che anima l'internet delle cose, dei giocattoli, dei corpi, che consente di usufruire di assistenti domestici robotizzati o di dispositivi per la sanità in rete.

Non soltanto perché i dati personali sono il "motore" dell'intelligenza artificiale, ma anche e soprattutto perché la disciplina di protezione dati, pur tecnologicamente neutra, è il settore normativo più avanzato e maggiormente capace di governare la complessità della società digitale, nel rispetto della dignità della persona.

Dall'esattezza dei dati utilizzati e dalla logica del trattamento alla base della configurazione degli algoritmi dipende l'"intelligenza" delle loro scelte.

Se è errata la classificazione delle casistiche di riferimento fornita all'algoritmo per decidere, ad esempio, la natura di una patologia o per valutare un marker, sarà poi la conseguente diagnosi ad essere sbagliata, con effetti potenzialmente anche fatali per il paziente.

Le possibili implicazioni, sul piano sociale, sono tutt'altro che marginali.

Gli algoritmi non sono neutri sillogismi di calcolo, ma opinioni umane strutturate in forma matematica che, come tali, riflettono, in misura più o meno rilevante, le precomprensioni di chi li progetta, rischiando di volgere la discriminazione algoritmica in discriminazione sociale.

Rispetto a questi rischi, risultano importanti le garanzie sancite dal nuovo quadro giuridico in ordine ai processi decisionali automatizzati, assicurandone la contestabilità e la trasparenza della logica, ed esigendo, almeno in ultima istanza, il filtro dell'uomo, per contrastare la delega incondizionata al cieco determinismo della tecnologia.

Oltre al diritto alla trasparenza delle scelte algoritmiche, altrimenti opache e insindacabili, il legislatore ha poi opportunamente valorizzato - con la sanzione penale - la tutela rispetto ad utilizzi discriminatori della profilazione, in particolare basata su dati sensibili, nel contesto delle attività investigative.

Al di là del quasi ancestrale timore di un uomo vittima delle sue creazioni, emerge quindi il bisogno di fondare basi etiche e giuridiche solide per uno sviluppo davvero sostenibile, perché la tecnologia deve poter servire e integrare, senza sostituire, l'intelligenza umana.

Le regole di protezione dati, se inscritte negli algoritmi assieme ai principi di precauzione, tutela della dignità umana "*by design*", possono ispirarne "l'intelligenza", nella direzione di un nuovo umanesimo digitale.

Del resto, se l'Europa giocherà un ruolo importante in questa partita, sarà non tanto e non solo per gli investimenti e le risorse che stanzierà, quanto per la capacità di dirigere l'innovazione in modo da coniugare etica e tecnica, libertà e algoritmi, mettendoli al servizio dell'uomo secondo quel "principio di responsabilità" indispensabile per governare il futuro.

L'applicabilità del nuovo quadro giuridico anche a trattamenti svolti da soggetti collocati al di fuori dell'Unione europea, ma con un impatto rilevante per i cittadini europei, segna una conquista fondamentale.

Costringendo anche le imprese non europee ad adeguarvisi, questa disciplina stimola infatti una vera e propria convergenza globale sui suoi principi e sul suo modo di coniugare innovazione e dignità umana, che si sta rivelando vincente nel contesto attuale, se è vero che un numero crescente di Paesi stanno adottando normative simili.

È auspicabile che questa convergenza rappresenti il primo passo per il riconoscimento universale del diritto alla protezione dati quale diritto fondamentale della persona, oltre che necessario presupposto di democrazia.

Giustizia, sicurezza pubblica e nazionale

Un'importante innovazione conseguente al nuovo quadro giuridico concerne l'attrazione dei trattamenti svolti a fini di prevenzione, accertamento e repressione dei reati, nell'ambito di applicazione della direttiva 680/2016, il cui decreto di recepimento ha introdotto alcune norme di rilievo.

Si pensi, in particolare, alla previsione del diritto del terzo a ottenere, anche nel processo, la rettifica, cancellazione o limitazione dei suoi dati contenuti in atti giudiziari o della sanzione penale per gli abusi del potere di trattamento dei dati dei cittadini.

In questa circostanza, consideriamo un'occasione mancata l'omessa modifica della disciplina sulla conservazione, per fini di giustizia, dei dati di traffico telefonico e telematico in senso conforme alla giurisprudenza della Corte di giustizia, con l'abrogazione della norma sulla conservazione per sei anni dei tabulati.

La loro conservazione per un periodo così lungo, indifferenziata per tipologia di dati e presupposti d'indagine, contrasta infatti con il principio di proporzionalità tra limitazione della riservatezza ed esigenze investigative.

È stato altresì reso parere sul decreto legislativo in materia di intercettazioni, con la richiesta di un rafforzamento delle cautele nell'esecuzione degli ascolti mediante captatore.

Pur recependo solo alcune delle nostre osservazioni, il testo definitivo del decreto introduce comunque innovazioni importanti, limitando - sotto il controllo del pubblico ministero - l'ingresso nel fascicolo processuale di conversazioni irrilevanti, così rafforzando le garanzie di riservatezza soprattutto dei terzi, nel rispetto del contraddittorio e senza per questo indebolire i poteri investigativi.

Le difficoltà che si stanno riscontrando nell'attuazione del decreto vanno dunque affrontate con tutto l'impegno che meritano, ma auspichiamo non inducano ad abbandonare i principi fondanti una riforma che contribuisce a coniugare privacy ed esigenze di giustizia.

In ordine ai trattamenti per fini di sicurezza nazionale è stato rinnovato il

protocollo d'intenti tra Autorità Garante e DIS, che rilancia le linee dell'intesa istituzionale avviata nel 2013, riferendola anche al nuovo dPCM in materia di *cybersecurity*.

Contesto in cui, del resto, il legislatore europeo ha instaurato una significativa simmetria tra protezione dati e sicurezza cibernetica, particolarmente evidente in alcuni istituti che accomunano il Regolamento e la direttiva NIS.

Del resto una normativa, che fa della protezione dei dati e dei sistemi dal rischio informatico il suo fulcro essenziale, non può che promuovere quelle condizioni complessive di tutela indispensabili per la sicurezza cibernetica.

La responsabilizzazione di imprese e pubbliche amministrazioni promossa dal Regolamento, rispetto al rischio "sociale" derivante da sistemi informatici permeabili rappresenta, in questo senso, una risorsa preziosa - anche di tipo reputazionale - e, non a caso, valorizzata anche dalla normativa in materia di *cybersecurity*.

Libertà di espressione, dignità, informazione

Nella società disintermediata ciascuno diviene al tempo stesso fruitore e produttore di informazione, con un indubbio potenziamento della libertà di espressione ma con il rischio, per converso, di una generale sottovalutazione dell'importanza dell'attendibilità delle notizie diffuse, della loro qualità, esattezza, correttezza. A farne le spese sono spesso i bersagli dell'*hate speech* o di campagne diffamatorie, scelti generalmente quali capri espiatori in ragione di proprie vulnerabilità. In tale contesto, il ruolo del giornalista si carica ulteriormente di responsabilità nel fornire un'informazione corretta e rispettosa dei diritti altrui: un faro da seguire per orientarsi tra le post-verità.

La protezione dati deve rappresentare, in questo senso, uno dei criteri regolativi essenziali per l'attività giornalistica: il necessario complemento di un'informazione tanto libera e indipendente, quanto rispettosa della dignità della persona.

Quest'auspicio, in particolare, ha ispirato una intensa interlocuzione con gli organi d'informazione, alla quale spesso è seguita l'adesione spontanea di testate o blog. È stato tuttavia necessario rivolgere all'Ordine dei giornalisti un monito al rispetto del principio di non discriminazione e del diritto all'anonimato del minore, a seguito di un eccesso di dettagli riscontrato in relazione ad alcuni fatti di cronaca.

Di particolare rilievo è risultata anche l'attività volta ad accordare tutela ai minori vittime di cyberbullismo. Se nella maggior parte dei casi è stato rimosso il contenuto lesivo a seguito dell'intervento del Garante o per spontanea adesione dei gestori, le maggiori criticità si sono riscontrate rispetto a siti extraeuropei.

In materia di "diritto all'oblio" si sono affermati principi importanti, tali da rafforzare incisivamente le tutele dell'interessato. Rileva in tal senso, ad esempio, la decisione sulle richieste di deindicizzazione globale (estesa quindi anche alle versioni extraeuropee dei motori di ricerca), attualmente all'esame della Corte di giustizia e risolta dal Garante nel senso dell'ammissibilità.

Con alcune decisioni, abbiamo voluto ampliare la tutela, includendo, tra i parametri di ricerca delle notizie da deindicizzare, anche specifici attributi personali, ulteriori rispetto al nominativo, volti a meglio specificare l'identità (generalmente sotto il profilo professionale) dell'interessato.

In tal modo, si è inteso impedire che l'"oblio" accordato rispetto alle notizie ricavabili a partire dal nominativo, possa essere vanificato aggiungendo, nella stringa di ricerca, anche soltanto un termine ulteriore: risultato che sarebbe contrario ai principi sanciti con la sentenza Costeja.

I primi accertamenti condotti, in cooperazione con le altre Autorità, sul caso Cambridge Analytica-Facebook, hanno messo in luce le implicazioni, spesso sottovalutate, del sistema di gestione delle inserzioni sulle grandi piattaforme del web. Esso determina, infatti, un flusso di dati degli utenti verso innumerevoli

"terze parti" poco trasparente e, nella maggior parte dei casi, del tutto ignorato dagli interessati. È, questa, una frontiera aperta su cui le Autorità di protezione dati interverranno, presumibilmente a lungo, avvalendosi dei nuovi strumenti loro riconosciuti - anche rispetto agli OTT - dal Regolamento generale e dal Regolamento e-privacy.

E-voting, propaganda elettorale, lavoro

Il processo di digitalizzazione investe anche l'attività politica, creando indubbi vantaggi ma anche rischi, spesso sottovalutati.

Significative, in questo senso, le vulnerabilità riscontrate in una piattaforma di partecipazione politica, già interessata da un *data breach*, rispetto alla quale il Garante ha prescritto le misure necessarie a rafforzare le garanzie di sicurezza dei dati trattati.

Si è inoltre richiesto di procedere all'anonimizzazione dei dati relativi alla espressione del voto al termine delle relative operazioni, riconfigurando il sistema di *e-voting* secondo misure di *privacy by default*.

In ordine alla propaganda elettorale via sms ed e-mail, sono state invece riscontrate alcune illiceità nell'attività svolte da un partito, a livello nazionale e locale, nonché l'indebito utilizzo da parte di un ex assessore, a fini propagandistici, di indirizzi e-mail acquisiti nell'esercizio del mandato, per il diverso fine dell'assolvimento delle proprie funzioni.

E se l'utilizzo delle nuove tecnologie nell'attività politica va corredato dalle misure necessarie a impedire l'indebita rivelazione di dati sensibili, quali quelli sull'adesione a partiti o movimenti, in un settore come quello del lavoro esso rischia di rappresentare - se non bilanciato da adeguate cautele - un potenziale fattore di ulteriore squilibrio del rapporto lavorativo.

Qui il pericolo maggiore non è tanto e non è solo la sostituzione del dipen-

dente con la macchina che "gli ruberebbe il lavoro", quanto piuttosto la robotizzazione dell'uomo-lavoratore.

Emergono nuovi tipi di lavoro, attratti nella categoria generale della *gig economy* e, come nel caso dei *riders*, sempre più inscritti in un rapporto strettissimo tra uomo e algoritmo, in cui è il secondo a impartire direttive al primo, privato persino della relazione interpersonale con un datore di lavoro, verso il quale esercitare i propri diritti.

In tale contesto, caratterizzato peraltro dalla sottoposizione del lavoratore a inedite quanto pervasive forme di controllo, la protezione dati assurge a presupposto necessario di libertà del lavoratore nell'esecuzione della prestazione, nonché fattore di riequilibrio di un rapporto di forza sempre più sbilanciato.

Muovono da questa consapevolezza alcune recenti sentenze della Cedu, volte a ribadire, in particolare, l'esigenza di una significativa gradualità nei controlli datoriali e la puntuale informazione del lavoratore in ordine alle loro caratteristiche.

Ancora, in relazione alla sempre più diffusa videosorveglianza nei luoghi di lavoro, la Corte ha precisato come la legittima aspettativa di riservatezza del lavoratore non possa venir meno in ragione del mero carattere pubblico del luogo in cui si svolge la prestazione lavorativa.

Questi principi hanno ispirato, tra gli altri, l'Autorità nell'interpretazione della disciplina dei controlli sul lavoro, come modificata dal Jobs Act.

In questo senso, ad esempio, i sistemi di geolocalizzazione (installati anche su smartphone o tablet) sono stati ritenuti in linea prevalente non qualificabili quali strumenti direttamente preordinati all'esecuzione della prestazione lavorativa, con conseguente applicazione della procedura concertativa o autorizzatoria prevista per i controlli a distanza.

Abbiamo riconosciuto la stessa qualificazione al sistema adottato, negli uffici postali, per gestire la coda agli sportelli, con modalità tali da consentire

anche il monitoraggio pervasivo e costante dei dipendenti e per questo, tra l'altro, dichiarato illecito e conseguentemente vietato.

In questo caso è stato accertato, in particolare, che la "consolle di monitoraggio" funzionale all'attivazione di tale sistema consentiva a oltre 12.000 soggetti incaricati di accedere in via continuativa (memorizzare ed estrarre anche in report individuali) ai dati inerenti tutti gli operatori in servizio, in qualunque momento, presso un determinato ufficio.

Tale esteso monitoraggio è risultato, tra l'altro, incompatibile con il principio di proporzionalità che deve regolare il rapporto tra esigenze datoriali e privacy del lavoratore, per impedire che la tecnologia rappresenti un fattore di regressione volto a comprimere, anziché espandere, le libertà.

Telemarketing

Un impegno straordinario è stato profuso anche quest'anno nelle attività di contrasto del telemarketing selvaggio, con controlli effettuati, anche al di fuori dei confini nazionali, nei confronti di una pluralità di soggetti operanti in questa filiera: dai principali committenti (in particolare, operatori telefonici e del mercato energetico) fino agli "ultimi anelli della catena" costituita - non di rado - da operatori di call center con capitali sociali pari a poche migliaia di euro.

Le verifiche ispettive *in loco*, realizzate con il supporto del Nucleo privacy della Guardia di Finanza - che ringrazio per la consolidata essenziale collaborazione - hanno fatto emergere un utilizzo spregiudicato di ingenti basi di dati di utenze telefoniche (anche di dubbia origine), l'assenza di adeguate procedure di raffronto con le doverose *black list*, la violazione delle regole di correttezza nella raccolta del consenso e una generalizzata noncuranza nei riguardi dei diritti degli interessati.

L'accertamento di numerosissimi contatti commerciali effettuati in violazione di legge ha condotto all'adozione di provvedimenti correttivi assai articolati, nonché all'irrogazione di sanzioni tra le più elevate.

Emerge un intricato reticolo di interessi poco chiari e relazioni non sempre formalizzate tra committenti, agenti e innumerevoli call center, nonché il fenomeno di chiamate promozionali da numerazioni "fantasma" assegnate a soggetti non identificabili, o - a detta dei committenti - non appartenenti alla propria rete di vendita, ancorché i contatti commerciali siano attivati nel loro interesse.

Abbiamo avuto una proficua interlocuzione con il Parlamento, ai fini della predisposizione della nuova disciplina del Registro delle opposizioni, che auspichiamo possa assicurare l'effettività delle garanzie per gli interessati.

L'Autorità continuerà, in ogni caso, a contrastare con decisione ogni tipo di illecito.

Sanità

Costante è l'attenzione dell'Autorità ai trattamenti svolti in ambito sanitario.

In proposito, in occasione dell'esame di un progetto proposto alla Regione Lombardia, che prevede un trattamento ulteriore, per fini di ricerca, dei dati sanitari dei pazienti, abbiamo auspicato un chiarimento nell'articolazione dei rapporti tra soggetti pubblici e aziende coinvolte nella sperimentazione. È stato altresì evidenziato come nel contesto in cui si sperimentano tecniche innovative basate sull'intelligenza artificiale, coinvolgendo una cospicua parte della popolazione, non si possa prescindere da una ponderata valutazione di impatto sulla protezione dei dati.

L'impiego delle nuove tecnologie nel campo della ricerca medico-scientifica è infatti, anzitutto, un fattore di sviluppo e di benessere collettivo e come tale va promosso, senza tuttavia rinunciare alla piena tutela dei diritti delle persone.

Ci siamo poi adoperati per promuovere il rispetto dei nuovi obblighi vaccinali, favorendo lo scambio dei dati dei minori tra scuole e aziende sanitarie. E rispetto alla disciplina da seguire a regime, abbiamo suggerito la previsione di modalità operative più idonee a ridurre i rischi per gli interessati, garantendo l'essenzialità e la sicurezza dei dati trasmessi.

Il processo di trasformazione digitale della sanità continua a presentare non poche vulnerabilità e carenze in termini di sicurezza. Significativi in tal senso alcuni *data breach* - che hanno talora reso possibile visualizzare le prestazioni mediche di altri assistiti - rispetto ai quali siamo intervenuti con provvedimenti prescrittivi e sanzionatori.

Infine, a fronte di una richiesta, avanzata da una struttura sanitaria, di autorizzazione a informare i congiunti della condizione di sieropositività di un paziente, abbiamo rilevato come tale comunicazione non possa prescindere dal coinvolgimento dell'interessato, che va sensibilizzato, non solo in ordine alle possibili responsabilità penali, quanto in ordine ai rischi ai quali potrebbe esporre il partner con comportamenti scorretti.

L'assenza di obbligo legale di informazione ai congiunti sulla condizione di sieropositività del paziente è, del resto, funzionale a impedire che il timore di tale comunicazione induca, nei cittadini, atteggiamenti difensivi ostacolando la diagnosi - e la conseguente terapia - di tali patologie.

La riservatezza del dato sanitario rappresenta dunque, soprattutto in tali circostanze, anche un necessario presupposto della corretta relazione fiduciaria tra medico e paziente.

Trasparenza e banche dati pubbliche

Sul versante della trasparenza, l'Autorità è stata chiamata, in particolare, a pronunciarsi su diversi casi di accesso civico generalizzato, consolidando un indirizzo interpretativo particolarmente rilevante in ordine al bilanciamento fra tutela dei dati personali e trasparenza.

Tra i molti casi esaminati, rileva in particolare quello inerente la richiesta di copia dei provvedimenti giudiziari di condanna al pagamento di somme in favore di un Comune, emessi negli ultimi cinque anni o anche precedentemente, se inadempiuti.

Il Garante ha ritenuto legittima la scelta di concedere un quadro riassuntivo riportante gli elementi di interesse pubblico dei provvedimenti giudiziari ma non la loro copia integrale, comprensiva di dati anche sensibili degli interessati.

Il carattere pubblico della sentenza e del processo non implica infatti, per ciò solo, la conoscibilità da parte di chiunque, delle generalità, con tutti i dettagli delle personali vicende, dei soggetti a vario titolo coinvolti nel giudizio.

In un altro caso, è stato ritenuto inammissibile l'accesso civico a dati identificativi di beneficiari di provvedimenti di concessione di sovvenzioni o sussidi, ove se ne possa evincere la condizione di disagio economico-sociale, in conformità al divieto, espressamente previsto, di diffusione di tali dati per fini di trasparenza.

L'incidente occorso alla piattaforma telematica dedicata allo Spesometro, contenente i dati fiscali di milioni di contribuenti, ha fornito invece l'occasione per segnalare al Governo quanto rilevanti possano essere i rischi derivanti dalla gestione dei sistemi informativi, in assenza di un adeguata attenzione agli aspetti di sicurezza e protezione dei dati personali.

A fronte della necessità di ricorrere sempre più allo scambio telematico dei dati e all interconnessione dei sistemi informativi pubblici, si riscontra l'esigenza di una maggiore consapevolezza e di competenze idonee a fronteggiare l'incremento dei rischi, suscettibili di derivarne, per i diritti dei cittadini.

All'aumento di tali rischi dovrebbe, infatti, corrispondere una costante attenzione nella gestione dei sistemi informativi e un crescente impegno nell'osservanza degli obblighi di sicurezza e di qualità dei dati, di cui i soggetti pubblici devono farsi carico.

In questo quadro, abbiamo sollecitato una forte iniziativa, da parte delle diverse istituzioni coinvolte nei processi decisionali relativi all innovazione tecnologica del Paese, per una verifica puntuale dello stato di sicurezza delle banche dati pubbliche e dei processi in corso di attuazione dell Agenda digitale.

Sotto questo profilo, abbiamo segnalato che alcune recenti norme volte alla duplicazione e integrazione generalizzata delle banche dati delle pubbliche amministrazioni, contrastano con i principi, di matrice europea, di proporzionalità, non eccedenza, limitazione della finalità.

La pur necessaria valorizzazione del patrimonio informativo pubblico non deve avvenire a discapito della tutela dei diritti fondamentali e con possibili ricadute anche in termini di sicurezza nazionale.

Pertanto, eserciteremo con responsabilità il nostro ruolo affinché tali iniziative non comportino per i cittadini italiani un arretramento dell'effettività dei principi europei su cui si fonda la salvaguardia dei dati personali.

In questi anni, l'Autorità è stata un punto di riferimento importante per le nuove esigenze di tutela dettate dai cambiamenti che hanno segnato questa complessa stagione.

Cercheremo di esserlo anche in futuro, valorizzando al massimo gli strumenti offerti dal nuovo quadro giuridico europeo e dal decreto di adeguamento, sul cui schema - tanto in sede di audizione quanto di parere - abbiamo suggerito modifiche volte a rafforzare le garanzie dei cittadini, negli spazi di flessibilità concessi dal legislatore europeo.

È stata avanzata da più parti la richiesta di un periodo di astensione dall'esercizio della potestà sanzionatoria. Ovviamente è una prospettiva non compatibile con il Regolamento, oltre che tale da privare la collettività dell'efficacia deterrente, propria di tali sanzioni, rispetto a violazioni anche gravi dei diritti delle persone.

Tuttavia, come già affermato anche in sede di audizione parlamentare sullo schema di decreto legislativo di adeguamento al GDPR, orienteremo, secondo criteri di gradualità, l'attività ispettiva e sanzionatoria sui trattamenti maggiormente rilevanti per dimensioni e concentrazione di dati, nonché per la loro rischiosità.

Le sfide che nei prossimi anni dovremo vincere ogni giorno si giocano nell'esercizio di questo straordinario diritto di libertà, ma si proiettano molto al di là, lungo orizzonti che ora possiamo solo intravedere.

Percorreremo questa strada con il senso di responsabilità che ha sempre caratterizzato la nostra azione e per cui, guardando a ritroso, sento di dover rivolgere un particolare ringraziamento al Segretario generale e a tutti coloro che, nell'Ufficio, si impegnano costantemente con dedizione e professionalità, in un'attività tanto affascinante quanto complessa.

E ringrazio davvero le Colleghe Augusta Iannini, Giovanna Bianchi Clerici, Licia Califano, componenti il Collegio del Garante: con loro abbiamo condiviso scelte importanti e decisioni significative, all'esito di confronti che hanno indubbiamente arricchito noi stessi e l'Autorità.

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

stampa:
Tipolitografia Ugo Quintily S.p.A.

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

www.garanteprivacy.it